ECORD
AND
RIEFS.

Supreme Court, U.S.
FILED
DEC 22 2016
OFFICE OF THE CLERK

No. 15-1194

IN THE

Supreme Court of the United States

LESTER GERARD PACKINGHAM,

Petitioner,

v.

NORTH CAROLINA,

Respondent.

On Writ of Certiorari to the
Supreme Court of North Carolina

BRIEF OF *AMICI CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER (EPIC), THIRTY TECHNICAL EXPERTS AND LEGAL SCHOLARS, AND FIVE PRIVACY AND CIVIL LIBERTIES ORGANIZATIONS IN SUPPORT OF PETITIONER

MARC ROTENBERG
Counsel of Record
ALAN BUTLER
ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
rotenberg@epic.org

December 22, 2016

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

INTEREST OF THE *AMICI CURIAE* 1
Technical Experts and Legal Scholars 2
Privacy and Civil Liberties Organizations 4

SUMMARY OF THE ARGUMENT 7

ARGUMENT 8
I. The First Amendment Protects the Right to Access Speech from the Privacy of a Personal Electronic Device 8
A. The Freedom of Speech Includes the Right to Pursue Information and Ideas Without Government Interference 9
B. Today's 'Private Library' Includes Information and Ideas Accessed on a Personal Electronic Device 13
C. North Carolina's Statute Hides a Breathtaking Amount of Speech From the View of Released Offenders 18
II. Laws That Rely on Dragnet Surveillance of Online Speech Threaten Privacy and Free Expression 23
A. Section 14.202.5, Which Asks Police to Find Needles in Haystacks, Cannot be Implemented Without Large-Scale Monitoring of Online Speech 24
B. Social Media Monitoring Chills Free Expression and Invades the Privacy of All Users 28

CONCLUSION 31

TABLE OF AUTHORITIES

CASES

Allentown Mack Sales & Serv., Inc. v. NLRB,
522 U.S. 359 (1998) 10

Ashcroft v. ACLU,
542 U.S. 656 (2004) 16

Ashcroft v. Free Speech Coal.,
535 U.S. 234 (2002) 10

Bd. of Educ., Island Trees Union Free Sch. Dist. No. 26 v. Pico,
457 U.S. 853 (1982) 10, 11, 13

Brown v. Entm't Merchants Ass'n,
564 U.S. 786 (2011) 22

Doe v. City of Albuquerque,
667 F.3d 1111 (10th Cir. 2012) 22

First National Bank of Boston v. Bellotti,
435 U.S. 765 (1978) 10

Florida v. Jardines,
133 S. Ct. 1409 (2013)
(Kagan, J., concurring) 17

Jacobson v. United States,
503 U.S. 540 (1992) 8

Kleindienst v. Mandel,
408 U.S. 753 (1972) 10

Lamont v. Postmaster General,
381 U.S. 301 (1965)
(Brennan, J., concurring) 11

Martin v. Struthers,
319 U.S. 141 (1943) 10

NASA v. Nelson,
562 U.S. 134 (2011) 28

Olmstead v. United States,
277 U.S. 438 (1928)
(Brandeis, J., dissenting) 11

Reno v. ACLU,
521 U.S. 844 (1997) 8, 15, 16, 23

Riley v. California,
134 S. Ct. 2473 (2014) 9, 16, 17

Sorrell v. IMS Health Inc.,
564 U.S. 552 (2011) 9

Stanley v. Georgia,
394 U.S. 557 (1969) 7, 8, 9, 12, 13, 18, 28

United States v. Di Re,
332 U.S. 581 (1948) 28

United States v. Jones,
132 S. Ct. 945 (2012)
(Sotomayor, J., concurring) 28

United States v. Playboy Entm't Grp., Inc.,
529 U.S. 803 (2000) 13

United States v. Stevens,
559 U.S. 460 (2010) 21

Webster v. Reprod. Health Servs.,
492 U.S. 490 (1989) 11

STATUTES

N.C. Gen. Stat § 14.202.5 ..... 7, 18, 19, 22, 24

OTHER AUTHORITIES

A. Michael Froomkin, *Pseudonyms by Another Name: Identity Management in a Time of Surveillance, in Privacy in the Modern Age* (Marc Rotenberg, Julia Horwitz, & Jeramie Scott eds., 2015) 30

Andrew Perrin & Maeve Duggan, *Americans' Internet Access: 2000-2015*, Pew Research Center (June 26, 2015) 15

Anita L. Allen & Marc Rotenberg, *Privacy Law and Society* (3d ed. 2016) 12

CNN Service Agreement, CNN.com (Sept. 24, 2015) 20

DHS Monitoring of Social Networking and Media: Enhancing Intelligence Gathering and Ensuring Privacy: Hearing Before the Subcomm. on Counterterrorism & Intelligence of the H. Comm. on Homeland Sec., 112th Cong. 2 (2012) (statement of Rep. Patrick Meehan, Chairman, Subcomm. on Counterterrorism & Intelligence) 27

Edit Profile, The New York Times 19

EPIC v. Department of Homeland Security: Media Monitoring, EPIC 26

Help: Comments, The New York Times 19

How It Works, Geofeedia 27

IMDb Conditions of Use, IMDb 21

Jan Ransom, *Boston Police Set to Buy Social Media Monitoring Software*, Boston Globe (Nov. 26, 2016) 26

Jeffrey Rosen, *The Deciders: Facebook, Google, and the Future of Privacy and Free Speech, in Constitution 3.0* (Jeffrey Rosen & Benjamin Wittes eds., 2011) 23

Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 Stan. L. Rev. 1193 (1998) 14

Julie E. Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (2012) 29

Kristine Lu & Jesse Holcomb, *Digital News Audience: Fact Sheet*, Pew Research Center (June 15, 2016) 15

Lee Rainie & Andew Perrin, *Slightly Fewer Americans Are Reading Rrint Books, New Survey Finds*, Pew Research Center (Oct. 19, 2015)..... 15

Limited Source Justification, Requisition Number: DJF-17-1300-PR-0000555, Federal Bureau of Investigation (Nov. 8, 2016) 25

Marc Jonathan Blitz, *Stanley in Cyberspace: Why the Privacy Protection of the First Amendment Should Be More Like That of the Fourth*, 62 Hastings L.J. 357 (2010)..... 14

Marc Rotenberg, Letter to the Editor, *Criticism 'Bombs'*, Boston Herald (Oct. 14, 2016)..... 26

Nadine Strossen, *Protecting Privacy and Free Speech in Cyberspace*, 89 Geo. L.J. 2103 (2001) 11

Offender Statistics, North Carolina Department of Public Safety..... 24

Purchase Order Records for Purchases of Social Media Monitoring Software by State and Local Governments, Brennan Center for Justice (Nov. 14, 2016)..... 27

Reddit user agreement, Reddit (May 27, 2016)..... 21

Report of the Chairman—Samuel Alito, *Conference on the Boundaries of Privacy in American Society*, Woodrow Wilson Sch. of Pub. & Int'l Affairs, Princeton Univ. (Jan. 4, 1972) 29

Scott Burns, *Already 1 Billion Websites, and Counting*, Houston Chronicle (Sept. 9, 2014) 9

Shannon Greenwood, Andrew Perrin, & Maeve Duggan, *Social Media Update 2016*, Pew Research Center (Nov. 11, 2016) 15

Terms of Service, LiveJournal (Dec. 12, 2010) 20

Terms of Service, Newsweek 20

Terms of Service, NYTimes.com (Nov. 15, 2015) 20

Terms of Service, Politico (July 11, 2016) 20

Terms of Service, Tumblr (Sept. 8, 2016) 20

Terms of Service, Washington Post (July 1, 2014) 20

Terms of Service, YouTube (June 9, 2010) 21

Terms of Use, Dribbble (Mar. 19, 2013) 21

Terms of Use, Last.fm (June 2, 2015) 21

The Library of Congress by the Numbers in 2015, Library of Congress (Feb. 1, 2016) 9

Tim Cushing, *Twitter Says Its API Can't Be Used For Surveillance, But What Does It Think The FBI's Going to Do With It?*, Techdirt (Nov. 22, 2016) 25

Welcome to MyHeritage, MyHeritage 21

Zeninjor Enwemeka, *Boston Police Plan To Buy Social Media Monitoring Software Draws Criticism*, WBUR News (Dec. 6. 2016) 26

INTEREST OF THE *AMICI CURIAE*

The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C.[1] EPIC was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other constitutional values.[2]

EPIC routinely participates as *amicus curiae* before this Court in cases concerning emerging privacy and civil liberties issues. *See, e.g.*, *amicus curiae* briefs of EPIC in *Utah v. Strieff*, 136 S. Ct. 2056 (2016) (arguing that evidence obtained via suspicionless identification should be suppressed); *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016) (arguing that the violation of a consumer's privacy rights under federal law constitutes an injury-in-fact sufficient to confer Article III standing); *City of Los Angeles v. Patel*, 135 S. Ct. 2443 (2015) (arguing that hotel guest registries should not be made available for inspection absent judicial review); *Riley v. California*, 134 S. Ct. 2473 (2014) (arguing that the of search a cell phone incident to arrest requires a warrant); *United States v. Jones*, 132 S. Ct. 945 (2012) (arguing that a warrant is required for the use of GPS tracking techniques); *Sorrell v. IMS Health*

---

[1] Both parties consent to the filing of this brief. In accordance with Rule 37.6, the undersigned states that no monetary contributions were made for the preparation or submission of this brief, and this brief was not authored, in whole or in part, by counsel for a party.

Inc., 564 U.S. 52 (2011) (arguing that the privacy interest in medical records justifies regulating data mining of prescription records); *Tolentino v. New York*, 562 U.S. 1043, (2010) (arguing that evidence obtained from defendant's identity should be suppressed when discovered as a result of an unlawful stop), *dismissed as improvidently granted*, 563 U.S. 123 (2011); *Doe v. Reed*, 561 U.S. 186 (2010) (arguing that state law should not force the disclosure of petition signatories); *Herring v. United States*, 555 U.S. 135 (2009) (arguing for the suppression of evidence obtained as the result of an error in a criminal justice database); *Hiibel v. Sixth Judicial Dist. Ct. of Nevada, Humboldt Cty.*, 542 U.S. 177 (2004) (arguing that identification may not be compelled absent probable cause to arrest); *Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Stratton, Ohio*, 536 U.S. 150 (2002) (arguing that door-to-door petitioners should not have to obtain a permit and identify themselves).

Technical Experts and Legal Scholars

Ann M. Bartow, Professor, Pace Law School

Colin J. Bennett, Professor, University of Victoria

Christine L. Borgman, Professor & Presidential Chair in Information Studies, UCLA

David Chaum, Chaum, LLC

Danielle Keats Citron, Morton & Sophia Macht Professor of Law, University of Maryland School of Law

Julie Cohen, Professor, Director of the Center on Privacy and Technology, Georgetown University Law Center

Dr. Whitfield Diffie, Consulting Scholar, Stanford Center for International Security and Cooperation

Laura Donohue, Professor, Director of the Center for National Security and the Law & Center on Privacy and Technology, Georgetown University Law Center

Addison Fischer, Founder and Chairman, Fischer International Corp.

Hon. David Flaherty, former Information and Privacy Commissioner for British Columbia

Deborah Hurley, Harvard University and Brown University

Ian Kerr, Canada Research Chair in Ethics, Law & Technology, University of Ottawa Faculty of Law

Harry R. Lewis, Gordon McKay Professor of Computer Science, Harvard University

Gary T. Marx, Professor Emeritus of Sociology, MIT

Mary Minow, Library Law Consultant

Eben Moglen, Professor of Law, Columbia Law School; Founding Director, Software Freedom Law Center

Dr. Pablo Garcia Molina, Adjunct Professor, Georgetown University

Dr. Peter G. Neumann, Computer Science Laboratory, SRI International

Dr. Deborah Peel, M.D., Founder and Chair, Patient Privacy Rights

Stephanie Perrin, President, Digital Discretion, Inc.

Chip Pitts, Lecturer in Law, Stanford Law School

Ronald L. Rivest, Professor of Electrical Engineering and Computer Science, MIT

Bruce Schneier, Security Technologist; Author, *Data and Goliath* (2015)

Dr. Barbara Simons, IBM Research (retired)

Robert Ellis Smith, Publisher, Privacy Journal

Nadine Strossen, John Marshall Harlan II Professor of Law, New York Law School; Former President, American Civil Liberties Union

Sherry Turkle, Abby Rockefeller Mauzé Professor of the Social Studies of Science and Technology, MIT

Edward G. Viltz, President and Chairman, Internet Collaboration Coalition

Christopher Wolf, Board Chair, Future of Privacy Forum

Shoshana Zuboff, Charles Edward Wilson Professor of Business Administration, Retired

(Affiliations are for identification only)

Privacy and Civil Liberties Organizations

Bill of Rights Defense Committee/Defending Dissent Foundation

The Bill of Rights Defense Committee/Defending Dissent Foundation is a national non-profit education and advocacy organization dedicated to fulfilling the promise of the Bill of Rights for everyone. We place a special emphasis on protecting the right to engage in political expression, as we were founded in 1960 by activists opposed to the activities of the House Un-American Activities Committee. As such, we are involved in defending the rights of individuals to read and receive materials on the internet freely and

curtailing the powers of the government to surveil social media and other online activity.

Center for Constitutional Rights

The Center for Constitutional Rights (CCR) is a national not-for-profit legal, educational, and advocacy organization dedicated to advancing and protecting the rights guaranteed by the United States Constitution and international human rights law. Founded in 1966 by attorneys who represented civil rights movements and activists in the South, CCR has protected the rights of marginalized groups for fifty years and has litigated historic First Amendment cases including *Dombrowski v. Pfister*, 380 U.S. 479 (1965), *Texas v. Johnson*, 491 U.S. 397 (1989), *United States v. Eichman*, 496 U.S. 310 (1990), and *Holder v. Humanitarian Law Project*, 561 U.S. 1 (2010). As such, CCR has an interest in ensuring that the government does not impose arbitrary restrictions on speech, particularly when such restrictions are based on disfavored status.

Consumer Action

Through multilingual financial education materials, community outreach, and issue-focused advocacy, Consumer Action empowers underrepresented consumers nationwide to assert their rights in the marketplace and financially prosper.

Freedom to Read Foundation

The Freedom to Read Foundation (FTRF) is an organization established by the American Library

Association to promote and defend First Amendment rights, foster libraries as institutions that fulfill the promise of the First Amendment, support the right of libraries to include in their collections and make available to the public any work they may legally acquire, and establish legal precedent for the freedom to read of all citizens.

National Center for Transgender Equality

The National Center for Transgender Equality (NCTE) is a national social justice organization founded in 2003 and devoted to advancing justice, opportunity and well-being for transgender people through education and advocacy on national issues.

SUMMARY OF THE ARGUMENT

The First Amendment protects not only the right to speak freely, but also the right to receive information and ideas. As this Court has explained, "If the First Amendment means anything, it means that a State has no business telling a man, sitting alone in his own house, what books he may read or what films he may watch." *Stanley v. Georgia*, 394 U.S. 557, 565 (1969). By dramatically limiting the range of news and social media websites that released sex offenders can access—sweeping far beyond any direct communication with minors—N.C. Gen. Stat § 14.202.5 runs roughshod over the freedom to access protected speech. The same First Amendment that protects the right to possess even legally obscene content in the home does not permit the state to prohibit access to some of the most widely used channels for protected speech. To hold otherwise would be in direct conflict with "the right to be let alone—the most comprehensive of rights and the right most valued by civilized man." *Stanley*, 394 U.S. at 564 (citing *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting)).

Nor is that the full extent of harms worked by section 14.202.5. For every website that released offenders are forbidden to visit, the statute creates a parallel incentive for the state to surveil. That is exactly how the instant case began: with police monitoring of a social media network. A statute that relies on dragnet surveillance of protected speech available to hundreds of millions internet users poses a grave threat to the privacy and free expression of all Internet users—not merely the offenders that the statute targets.

"Our whole constitutional heritage rebels at the thought of giving government the power to control men's minds." *Stanley*, 394 U.S. at 564. Yet that is precisely the effect this law promises to have.

ARGUMENT

I. The First Amendment Protects the Right to Access Speech from the Privacy of a Personal Electronic Device

Section 14.202.5 works a constitutional violation of staggering dimensions. The statute crudely sorts the "vast democratic forums of the Internet," *Reno v. ACLU*, 521 U.S. 844, 868 (1997), into two buckets: websites that are acceptable reading material for released offenders, and those that are not. If a website happens to allow users under 18 to register online, it is subject to the censor's pen, and no released offender may access *any* part of that website without fear of prosecution. This site-wide ban admits no exception, walling off news, debate, sports, scholarship, art, and every other shred of speech published under the same domain name.

Such an audacious restraint on the "right to receive information and ideas" cannot be squared with the First Amendment. *Stanley*, 394 U.S. at 564. A person's private reading preferences are entirely "his own and beyond the reach of government." *Jacobson v. United States*, 503 U.S. 540, 552 (1992). So robust is the freedom "to satisfy [one's] intellectual and emotional needs" in private that it extends even to speech which is unprotected in other settings. *Stanley*, 394 U.S. at 565.

North Carolina's statute flouts this right and impermissibly "dictate[s] to the mature adult what books he may have in his own private library." *Stanley*, 394 U.S. at 562 n.7 (quoting *State v. Mapp*, 166 N.E.2d 387, 393 (1960)). Indeed, the law reaches further than a conventional book ban ever could, tightening access to many of the billion-plus websites that populate the Internet and span the province of human knowledge. Scott Burns, *Already 1 Billion Websites, and Counting*, Houston Chronicle (Sept. 9, 2014).[3] Yet the state can no more criminalize what an individual chooses to read on a personal electronic device than it can restrict the contents of a home library: the privacy of both is sacrosanct. *Riley v. California*, 134 S. Ct. 2473, 2491 (2014) ("The possibility that a search might extend well beyond the papers and effects in the physical proximity of an arrestee is yet another reason that the privacy interests here dwarf those in *Robinson*.").

A. The Freedom of Speech Includes the Right to Pursue Information and Ideas Without Government Interference

Time and again, this Court has emphasized "that the Constitution protects the right to receive information and ideas." *Stanley*, 394 U.S. at 564; *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 568 (2011) (invalidating "a restriction on access to information

---

[3] http://www.chron.com/business/burns/article/Already-1-billion-websites-and-counting-5744910.php. By contrast, the Library of Congress contains only 162 million physical works. *The Library of Congress by the Numbers in 2015*, Library of Congress (Feb. 1, 2016), https://www.loc.gov/item/prn-16-023/.

in private hands" as a violation of the First Amendment); *Allentown Mack Sales & Serv., Inc. v. NLRB*, 522 U.S. 359, 386–87 (1998) ("Our decisions have concluded that First Amendment protection extends equally to the right to receive information . . . ."); *Bd. of Educ., Island Trees Union Free Sch. Dist. No. 26 v. Pico*, 457 U.S. 853, 867 (1982) (quoting *Stanley*, 394 U.S. at 564) ("[W]e have held that in a variety of contexts 'the Constitution protects the right to receive information and ideas.'"); *First National Bank of Boston v. Bellotti*, 435 U.S. 765, 783 (1978) (noting that the First Amendment protects "public access to discussion, debate, and the dissemination of information and ideas"); *Kleindienst v. Mandel*, 408 U.S. 753, 762 (1972) ("It is now well established that the Constitution protects the right to receive information and ideas."); *Martin v. Struthers*, 319 U.S. 141, 143 (1943) ("[The First Amendment] embraces the right to distribute literature and necessarily protects the right to receive it." (citation omitted)). "First Amendment freedoms are most in danger when the government seeks to control thought or to justify its laws for that impermissible end. The right to think is the beginning of freedom, and speech must be protected from the government because speech is the beginning of thought." *Ashcroft v. Free Speech Coal.*, 535 U.S. 234, 253 (2002).

The right to access information "is an inherent corollary of the rights of free speech and press" in two respects. *Pico*, 457 U.S. at 867. First, "the right to receive ideas follows ineluctably from the sender's First Amendment right to send them," *id.*, for "[i]t would be a barren marketplace of ideas that had only sellers and no buyers." *Lamont v. Postmaster General*, 381 U.S. 301, 308 (1965) (Brennan, J.,

concurring). Second, and "[m]ore importantly, the right to receive ideas is a necessary predicate to the *recipient*'s meaningful exercise of his own rights of speech, press, and political freedom." *Pico*, 457 U.S. at 867 (emphasis in original).

That right is all the more essential in the most intimate and familiar spaces of a person's life—those "private sphere[s]" which "the Constitution reserves from the intrusive reach of government." *Webster v. Reprod. Health Servs.*, 492 U.S. 490, 548 (1989). Writing almost a century ago, Justice Louis Brandeis reflected on the inseparable constitutional relationship between privacy and the right to pursue information and ideas:

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized man.

Olmstead, 277 U.S. at 478 (Brandeis, J., dissenting), *overruled in part by Katz v. United States*, 389 U.S. 347 (1967); *see also* Nadine Strossen, *Protecting Privacy and Free Speech in Cyberspace*, 89 Geo. L.J. 2103, 2105 (2001) ("[P]rominent champions of free speech rights have viewed privacy as the ultimate

bedrock of all our civil liberties, including our First Amendment rights."); Anita L. Allen & Marc Rotenberg, *Privacy Law and Society* 363 (3d ed. 2016) ("The First Amendment protects the mind's encounters with the sacred and the profane.").

In *Stanley*, this Court made clear that the right to "read or observe" materials in "the privacy of [one's] own home" is particularly far-reaching. *Stanley*, 394 U.S. at 564–65. Faced with a Georgia law that made "mere private possession of obscene matter" a crime, the Court deemed the premise of the statute "wholly inconsistent with the philosophy of the First Amendment." *Id.* at 565. The Court wrote:

> Whatever may be the justifications for other statutes regulating obscenity, we do not think they reach into the privacy of one's own home. If the First Amendment means anything, it means that a State has no business telling a man, sitting alone in his own house, what books he may read or what films he may watch. Our whole constitutional heritage rebels at the thought of giving government the power to control men's minds.

Id. The Court further explained that "the right to access information in private is so fundamental to our scheme of individual liberty, its restriction may not be justified by the need to ease the administration of otherwise valid criminal laws." *Id.* at 568. In other words: the right to receive ideas in private settings extends even farther than the ordinary sweep of the First Amendment, giving individuals the freedom to absorb speech that could

be permissibly suppressed in other contexts. *Id.* at 565; *see also United States v. Playboy Entm't Grp., Inc.*, 529 U.S. 803, 815 (2000) (noting the "First Amendment interests of speakers and willing listeners—listeners for whom, if the speech is unpopular or indecent, the privacy of their own homes may be the optimal place of receipt").

Of course, section 14.202.5 does not target unprotected categories of speech. Rather, it closes off vast, undifferentiated expanses of news and information. For example, the law bars access to entire websites, regardless of what type of information is being accessed or posted, merely because a person under 18 may create an account. It is difficult to conceive of a more brazen violation of the right to access ideas—or the right to be let alone—than this wholesale removal of works from an individual's digital library. As to such forms of censorship, this Court's precedents are unequivocal. "[T]he State may not, consistently with the spirit of the First Amendment, contract the spectrum of available knowledge," *Pico*, 457 U.S. at 866, for the "right to receive information and ideas, regardless of their social worth, is fundamental to our free society." *Stanley*, 394 U.S. at 564.

B. Today's 'Private Library' Includes Information and Ideas Accessed on a Personal Electronic Device

With the rise of the Internet and personal electronic devices, the composition of today's "private library" has changed dramatically since the days of *Stanley*. "[M]any of the cultural activities we engage in inside the home—reading, watching a video, surfing the Web—can now be performed in the

privacy of a digital home instead of a physical one." Marc Jonathan Blitz, *Stanley in Cyberspace: Why the Privacy Protection of the First Amendment Should Be More Like That of the Fourth*, 62 Hastings L.J. 357, 361 (2010). For example:

> Instead of relaxing in our living rooms, we might do so in the much more "spacious" living room of a virtual mansion we acquire in Second Life or another virtual world. Instead of buying a safe or chest to store paper documents in a closet, we might buy virtual space in the "cloud" of computer-based storage that numerous companies, such as Google, Apple, or Dropbox, provide for people to store digital files outside of their homes. Instead of buying and reading a physical book, many individuals armed with an eReader, an iPad, or another tablet computer might read a digital book . . . .

Id. at 361–62. *See also* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 Stan. L. Rev. 1193, 1195 (1998) ("The revolution in our communications infrastructure—in particular, the explosive growth of the Internet—has fundamentally transformed how we create, acquire, disseminate, and use information. . . . Now, digitized libraries make available vast resources, regardless of distance.").

The trend toward an ever-more digital personal library is ubiquitous. Some 84% of American adults now use the Internet. Andrew Perrin & Maeve

Duggan, *Americans' Internet Access: 2000-2015*, Pew Research Center (June 26, 2015).[4] "Nearly four-in-ten U.S. adults (38%) [say] that they often get news from digital sources, including news websites or apps (28%) and social networking sites (18%)." Kristine Lu & Jesse Holcomb, *Digital News Audience: Fact Sheet*, Pew Research Center (June 15, 2016).[5] Of Americans who are online, 79% access content on Facebook, and 76% of those users visit the site on a daily basis. Shannon Greenwood, Andrew Perrin, & Maeve Duggan, *Social Media Update 2016*, Pew Research Center (Nov. 11, 2016).[6] And while 63% of adult Americans say they still read at least one print book per year, 27% peruse an e-book and 12% listen to an audio book on an annual basis. Lee Rainie & Andew Perrin, *Slightly Fewer Americans Are Reading Rrint Books, New Survey Finds*, Pew Research Center (Oct. 19, 2015).

When this Court first addressed the issue of internet censorship in *Reno v. ACLU*, 521 U.S. 844 (1977), it recognized "adults have a constitutional right to receive" information online and "to address [that speech] to one another." 521 U.S. at 874. The Court struck down Congress's first attempt to restrict publication and transmission of indecent and patently offensive content online, in part because the statute was not sufficiently tailored and imposed a

---

[4] http://www.pewinternet.org/2015/06/26/americans-internet-access-2000-2015/.

[5] http://www.journalism.org/2016/06/15/digital-news-audience-fact-sheet/.

[6] http://www.pewinternet.org/2016/11/11/social-media-update-2016/.

burden on adults' intellectual freedom. *Id.* The government's attempt to regulate speech on the Internet—a medium "as diverse as human thought"—was tantamount to "burn[ing] the house to roast the pig" and threatened to "torch a large segment of the Internet community." *Id.* at 870, 882 (citation omitted).

Congress subsequently passed the Children's Online Protection Act ("COPA") in response to the Court's decision in *Reno*, and that statute was again enjoined by the Court in *Ashcroft v. ACLU*, 542 U.S. 656, 673 (2004), because it did not account for "less restrictive alternatives" and instead imposed "universal restrictions at the source." *Id.* at 673, 667.

More recently, this Court underscored the profoundly private nature of the information accessible through a personal electronic device. In *Riley v. California*, 134 S. Ct. 2473 (2014), the Court held that the Fourth Amendment bars warrantless searches of cell phones, even when undertaken for the general safety of arresting officers or to prevent the destruction of evidence. *Id.* at 2485. In reaching that conclusion, the Court described at length the ways in which a personal electronic device holds "the privacies of life," *id.* at 2495:

> First, a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's

> private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.

Id. at 2489. The Court continued:

> An Internet search and browsing history . . . can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns . . . . Indeed, a cell phone search would typically expose to the government far more than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.

Id. at 2490–91.

Taken together, *Stanley*, *Reno*, and *Riley* demonstrate that the right to access information on a personal electronic device is coextensive with the right to do so at home. In either instance, the state intrudes on "most intimate and familiar space[s]" of a person's life, *Florida v. Jardines*, 133 S. Ct. 1409, 1419 (2013) (Kagan, J., concurring), when it

"dictate[s] to the mature adult" what information he may access. *Stanley*, 394 U.S. at 562 n.7.

The government can no more tell a woman what websites she may access from the privacy of her computer than it can "tell[] a man, sitting alone in his own house, what books he may read." *Stanley*, 394 U.S. at 565. Section 14.202.5 offends the Constitution in exactly this way. By placing entire websites off limits to the private contemplation of released offenders, it attempts to do in a digital realm that which *Stanley* expressly prohibits in the home. Yet the First Amendment permits no such restraint on internet expression and no such invasion of a person's private thoughts.

C. North Carolina's Statute Hides a Breathtaking Amount of Speech From the View of Released Offenders

The alarming reach of section 14.202.5 is apparent from the many and varied websites that it censors. North Carolina's statute makes it a crime to "access a commercial social networking Web site where the sex offender knows that the site permits minor children to become members or to create or maintain personal Web pages." § 14.202.5(a). A "commercial social networking Web site" is defined as any website that satisfies four criteria: (1) the site must be "operated by a person who derives revenue from . . . the operation of the Web site"; (2) it must "[f]acilitate[] the social introduction between two or more persons"; (3) it must "[a]llow[] users to create Web pages or personal profiles"; **and** (4) it must "[p]rovide users or visitors . . . mechanisms to communicate with other users." § 14.202.5(b). Two narrow classes of websites are excluded: (1) any site

that "[p]rovides only one of the following discrete services: photo-sharing, electronic mail, instant messenger, or chat room or message board platform"; and (2) any site that "[h]as as its primary purpose the facilitation of commercial transactions involving goods or services between its members or visitors." § 14.202.5(c).

This is a strikingly broad definition of "commercial social networking Web site." Certainly a released offender may not visit Facebook or Myspace—provided he is aware that these websites permit minors to register—as both are squarely covered by section 14.202.5(b). But the prohibition extends much farther. Take, for example, the New York Times website, http://www.nytimes.com/, which is clearly a commercial site (thus satisfying the first requirement). Readers can post comments and responses to articles the day they are published (thus satisfying the second and fourth requirements).[7] These comments are linked to public profiles, which users create if they want to log in to the site (thus satisfying the third requirement).[8] The New York Times, and other similar news sites with comment

---

[7] *See, e.g.*, *Help: Comments*, The New York Times, *available at* http://www.nytimes.com/content/help/site/usercontent/usercontent.html#usercontent-closed (last visited Dec. 20, 2016).

[8] *See Edit Profile*, The New York Times, *available at* http://www.nytimes.com by logging in at the top right and selecting "Edit Profile" from the top right menu (last visited Dec. 20, 2016) ("Your profile is public. It will appear with any comments you leave with the NYTimes.com.")

threads and profiles, could thus qualify as commercial social media websites under the statute.

In addition, the New York Times and other similar sites typically allow minors to register and subscribe if they are "13 years or older." *Terms of Service*, NYTimes.com (Nov. 15, 2015).[9] As a result, Petitioner and other similarly situated individuals are barred from checking the latest online news from the New York Times, the Washington Post, Politico, Newsweek, or CNN. *See Terms of Service*, Washington Post (July 1, 2014);[10] *Terms of Service*, Politico (July 11, 2016);[11] *Terms of Service*, Newsweek;[12] *CNN Service Agreement*, CNN.com (Sept. 24, 2015).[13] Nor may he post his personal thoughts—or read the thoughts of others—on blogging platforms like Tumblr and LiveJournal, because they, too, rely on profiles and comment threads to facilitate social interactions. *Terms of Service*, Tumblr (Sept. 8, 2016);[14] *Terms of Service*, LiveJournal (Dec. 12, 2010).[15] He may not listen to music on Last.fm, or read discussion threads on Reddit, or look up an actor's name on IMDb because those sites also enable sharing and commenting for

---

[9] http://www.nytimes.com/content/help/rights/terms/terms-of-service.html.

[10] https://www.washingtonpost.com/terms-of-service/2011/11/18/gIQAldiYiN_story.html.

[11] http://www.politico.com/terms-of-service.

[12] http://www.newsweek.com/terms-service (last visited Dec. 14, 2016).

[13] http://www.cnn.com/2014/01/17/cnn-info/interactive-legal/.

[14] https://www.tumblr.com/policy/en/terms-of-service.

[15] http://www.livejournal.com/legal/tos.bml.

registered users. *Terms of Use*, Last.fm (June 2, 2015);[16] *Reddit user agreement*, Reddit (May 27, 2016);[17] *IMDb Conditions of Use*, IMDb.[18] These sites are not alone in facilitating social interactions because that has increasingly become a standard feature of modern commercial websites. For example, Petitioner may not explore the work of artists on Dribbble, or watch videos on YouTube, or explore his own ancestry on MyHeritage. *Terms of Use*, Dribbble (Mar. 19, 2013);[19] *Terms of Service*, YouTube (June 9, 2010);[20] *Welcome to MyHeritage*, MyHeritage.[21]

In short, section 14.202.5 radically reshapes the internet available to a released offender, placing enormous quantities of protected expression out of bounds. The statute does not even pretend to require a meaningful nexus between the expression that it censors and people it aims to protect: speech need only share a common domain name with "social networking" activity by minors in order to land on the statute's blacklist. Section 14.202.5 is thus fatally overbroad, in that "a substantial number of its applications are unconstitutional, judged in relation to the statute's plainly legitimate sweep." *United States v. Stevens*, 559 U.S. 460, 473 (2010). This overbreadth is compounded by the statute's puzzling

---

[16] http://www.last.fm/legal/terms.

[17] https://www.reddit.com/help/useragreement/.

[18] http://www.imdb.com/conditions (last visited Dec. 14, 2016).

[19] https://dribbble.com/termsz.

[20] https://www.youtube.com/static?template=terms.

[21] https://www.myheritage.com/FP/Company/popup-terms-conditions.php (last visited Dec. 14, 2016).

exclusion of single-use platforms, § 14.202.5(c)(1), which allows released offenders to access speech through email and chatrooms that they could not access on news and social networking websites. Such an exception leaves the statute "wildly underinclusive when judged against its asserted justification, . . . rais[ing] serious doubts about whether the government is in fact pursuing the interest it invokes." *Brown v. Entm't Merchants Ass'n*, 564 U.S. 786, 802 (2011).

The Tenth Circuit has previously rejected the logic of North Carolina's statute in the context of brick-and-mortar libraries. In *Doe v. City of Albuquerque*, 667 F.3d 1111 (10th Cir. 2012), the court considered an Albuquerque regulation that barred released offenders from all public libraries in the city. *Id.* at 1116. Noting that a library is "the quintessential locus of the receipt of information" whose "very purpose . . . is to aid in the acquisition of knowledge through reading, writing, and quiet contemplation," the court struck down the city's "wholesale ban on any and all access to public libraries" as a violation of the First Amendment. *Id.* at 1129, 1134 (citations omitted). The city had failed, the court wrote, to show "that its ban was narrowly tailored to serve its interest in providing a safe environment for library patrons." *Id.* at 1133–34.

Section 14.202.5 fares no better. If a state may not ban released offenders from *public* libraries, surely it may not bar them from accessing a wide range of websites from the privacy of their own homes and electronic devices. However laudable the state's goals, North Carolina cannot simply "burn the house to roast the pig" where speech is concerned.

Reno, 521 U.S. at 882. The First Amendment does not permit it.

II. Laws That Rely on Dragnet Surveillance of Online Speech Threaten Privacy and Free Expression

Section 14.202.5 curtails privacy and free speech in a second way: by inviting police to engage in large-scale monitoring of news and social media sites. In forbidding registered offenders to access web-based services, the statute effectively requires police to surveil the internet to monitor the use of suspect and non-suspect alike. Given the wide range of content subject to section 14.202.5, meaningful enforcement would be functionally impossible by other means.

But placing government in the role of permanent eavesdropper is highly corrosive to privacy and free expression on the internet. Faced with the knowledge that a prying official may collect and scrutinize the contents of their personal profiles, individuals will inevitably trend towards greater self-censorship. *See* Jeffrey Rosen, *The Deciders: Facebook, Google, and the Future of Privacy and Free Speech, in Constitution 3.0* at 72–73 (Jeffrey Rosen & Benjamin Wittes eds., 2011) (explaining how "ubiquitous surveillance" through Facebook might "violate[] the right to autonomy," just as "citizens in the Soviet Union were inhibited by ubiquitous surveillance from expressing and defining themselves"). Nor are these effects limited to the released offenders that section 14.202.5 targets: *all* internet users must bear the weight of its impact.

A. Section 14.202.5, Which Asks Police to Find Needles in Haystacks, Cannot be Implemented Without Large-Scale Monitoring of Online Speech

Though section 14.202.5 sweeps broadly, it operates simply. The statute defines a universe of "commercial social networking Web sites" and prohibits released offenders from accessing those websites (provided that an offender is aware that a particular site allows minors to register). § 14-202.5(a)-(b).

What this simplicity obscures, however, is the far-reaching government surveillance that the law necessitates. North Carolina's registry includes nearly 15,000 released offenders residing in-state and another 4,700 living out of state. *Offender Statistics*, North Carolina Department of Public Safety.[22] To meaningfully police such a large group of people—or even a tiny fraction thereof—for compliance with section 14.202.5 is impossible without large-scale monitoring of social media profiles, photos, and other content. Given the statute's sprawling reach, such surveillance could extend to dozens of major websites and an incalculable number of smaller ones, placing huge segments of the internet under the watchful eye of police.

This kind of surveillance is hardly far-fetched: it is exactly what led to Petitioner's arrest under section 14.202.5. At the time, an officer from the Durham Police Department had begun a probe "to

---

[22] http://sexoffender.ncsbi.gov/stats.aspx (last visited Dec. 14, 2016).

detect such sex offenders living in Durham who were illegally accessing commercial social networking Web sites." *North Carolina v. Packingham*, 777 S.E.2d 738, 742 (2015). It was during this dragnet search, conducted with no apparent particularized suspicion of wrongdoing, that the officer located Petitioner's photo linked to a pseudonymously registered account. *Id.*

An increasing number of police agencies have engaged in this troubling and controversial practice in recent years. For instance, the Federal Bureau of Investigation recently hired private firm Dataminr to persistently monitor the more than 500 million tweets posted on Twitter each day. *Limited Source Justification, Requisition Number: DJF-17-1300-PR-0000555*, Federal Bureau of Investigation (Nov. 8, 2016).[23] The announcement was greeted with well-earned skepticism. *See, e.g.*, Tim Cushing, *Twitter Says Its API Can't Be Used For Surveillance, But What Does It Think The FBI's Going to Do With It?*, Techdirt (Nov. 22, 2016) ("Given the agency's long history of engaging in surveillance of protected political activity, it's not much of a stretch to believe the FBI will use Dataminr's tools for the same ends.").[24]

Similarly, the Boston Police Department recently announced that it would spend up to $1.4 million on social media monitoring software. Jan

---

[23] *Available at* https://epic.org/privacy/fbi/Dataminr-Limited-Source-Justification.pdf.

[24] https://www.techdirt.com/articles/20161117/15480436077/twitter-says-api-cant-be-used-surveillance-what-does-it-think-fbis-going-to-do-with-it.shtml.

Ransom, *Boston Police Set to Buy Social Media Monitoring Software*, Boston Globe (Nov. 26, 2016).[25] The plan has drawn widespread criticism. *See, e.g.*, Zeninjor Enwemeka, *Boston Police Plan To Buy Social Media Monitoring Software Draws Criticism*, WBUR News (Dec. 6. 2016) ("[Taylor Campbell of Quincy] likened social media sites to a public square and said keeping watch on them could have 'a chilling effect on speech.'"); *see also* Marc Rotenberg, Letter to the Editor, *Criticism 'Bombs'*, Boston Herald (Oct. 14, 2016) ("As law enforcement agencies have developed imperfect tools for electronic surveillance more and more innocent people are falling under suspicion.").

And in 2012, a Freedom of Information Act lawsuit by EPIC revealed that the Department of Homeland Security was monitoring "online forums, blogs, public websites, and messages boards" and disseminating the results to law enforcement agencies and private companies. *EPIC v. Department of Homeland Security: Media Monitoring*, EPIC.[26] As a consequence, Congress undertook oversight hearings to rein in this practice. Representative Patrick Meehan, Chairman of the House Subcommittee on Counterterrorism and Intelligence, warned at the hearing that "collecting, analyzing, and disseminating private citizens' comments could have a chilling effect on individual privacy rights and

---

[25] https://www.bostonglobe.com/metro/2016/11/25/boston-police-set-buy-social-media-monitoring-software/Vswk24jmuBkuMmPbPY4iYI/story.html.

[26] https://epic.org/foia/epic-v-dhs-media-monitoring/ (last visited Dec. 14, 2016).

people's freedom of speech and dissent against their government." *DHS Monitoring of Social Networking and Media: Enhancing Intelligence Gathering and Ensuring Privacy: Hearing Before the Subcomm. on Counterterrorism & Intelligence of the H. Comm. on Homeland Sec.*, 112th Cong. 2 (2012) (statement of Rep. Patrick Meehan, Chairman, Subcomm. on Counterterrorism & Intelligence).[27]

North Carolina is not immune to this alarming trend. At least two entities—Durham County and the North Carolina Department of Justice—have spent over $20,000 apiece on subscriptions to the social tracking software Geofeedia. *Purchase Order Records for Purchases of Social Media Monitoring Software by State and Local Governments*, Brennan Center for Justice 9, 10 (Nov. 14, 2016).[28] Geofeedia describes itself as a "cloud-based, location-based intelligence platform" that lets subscribers "predict, analyze, and act on real-time social media content by location." *How It Works*, Geofeedia.[29] Two other North Carolina governments—Charlotte and Rocky Mount—have spent upwards of $14,000 each on Snaptrends, a similar tracking program. Brennan Center for Justice, *supra*, at 3, 6.

Such is the inevitable consequence of laws and policies that ask police to find needles in digital

---

[27] https://homeland.house.gov/files/02-16-12%20Meehan%20Open.pdf.

[28] https://www.brennancenter.org/sites/default/files/analysis/Purchase_Order_Records_for_Purchases_Social_Media_Monitoring_Software_State_Local_Govts.pdf.

[29] https://geofeedia.com/products/how-it-works/ (last visited Dec. 14, 2016).

haystacks: greater government tracking of online speech. Yet the First Amendment, and indeed "our whole constitutional heritage," bristles at this pervasive form of monitoring. *Stanley*, 394 U.S. at 564; *see United States v. Jones*, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) ("Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse."); *NASA v. Nelson*, 562 U.S. 134, 145 n.6 (2011) ("[T]he First Amendment has a penumbra where privacy is protected from governmental intrusion."); *United States v. Di Re*, 332 U.S. 581, 595 (1948) ("[T]he forefathers, after consulting the lessons of history, designed our Constitution to place obstacles in the way of a too permeating police surveillance, which they seemed to think was a greater danger to a free people than the escape of some criminals from punishment.").

B. Social Media Monitoring Chills Free Expression and Invades the Privacy of All Users

Of course, it is not just released offenders whose privacy and free speech suffer under the surveillance spurred by section 14.202.5. Any person—adult or minor—who uses a "commercial social networking Web site" may be subject to such monitoring.

By design, digital dragnets collect and analyze data from scores of individuals who have no connection to the matter being investigated. For example, if a police officer in North Carolina were to search through Facebook for a released offender

using the pseudonym John Smith, it would be difficult to find the right person (if at all) without scanning through the personal profiles of a great many John Smiths. And there is little reason to think that surveillance under section 14.202.5 would remain so narrowly targeted. The law covers an immense constellation of websites and thousands upon thousands of released offenders—far too much content to reliably monitor without the type of automated assistance that North Carolina governments are increasingly using. *See supra* Part II.A.

Whatever the precise tools used to enforce section 14.202.5, the effect of enforcement-by-surveillance is to curtail the privacy and discourage the free expression of *all* users on affected websites. It has long been recognized that "government has often used improper means to gather information about individuals who posed no threat either to their government or their fellow citizens." Report of the Chairman—Samuel Alito, *Conference on the Boundaries of Privacy in American Society*, Woodrow Wilson Sch. of Pub. & Int'l Affairs, Princeton Univ. at 8 (Jan. 4, 1972). The impact of such "panoptic surveillance" is severe, as Professor Julie Cohen describes: "In creating fixed records of presence, appearance, and behavior at particular places and times, surveillance constitutes institutional and social memory." Julie E. Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* 137 (2012). Professor Cohen goes on to conclude that "surveillance of online activities alters the experience of space in the same ways that surveillance of real places does." *Id.* at 143.

Yet, as Professor Michael Froomkin has noted, the average citizen "is almost defenseless" in the "environment of increasingly pervasive surveillance of communications, transactions, and movements." A. Michael Froomkin, *Pseudonyms by Another Name: Identity Management in a Time of Surveillance, in Privacy in the Modern Age* 63 (Marc Rotenberg, Julia Horwitz, & Jeramie Scott eds., 2015). That is why constitutional limits on programs that would require such broad-scale surveillance are so essential. Without such protections, individuals fall victim to a "spiral of silence" where "motivated by fear of isolation, [they] continuously monitor their environments to assess whether their beliefs align with or contradict majority opinion." Elizabeth Stoycheff, *Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring*, Journalism & Mass Comm. Q., March 2016, at 1.

***

The First Amendment protects the right to receive information and ideas—never more so than in private. By sharply limiting the speech that released offenders may access from a personal electronic device, section 14.202.5 works a blatant violation of that fundamental freedom. Further, by promoting across-the-board surveillance of news and social media websites, the statute imperils the privacy and free expression of all internet users. It should be struck down.

CONCLUSION

For the foregoing reasons, *amici* respectfully ask this Court to reverse the decision of the Supreme Court of North Carolina.

Respectfully submitted,

MARC ROTENBERG
ALAN BUTLER
ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
(202) 483-1248 (fax)
rotenberg@epic.org

December 22, 2016